


[Web](#) [Images](#) [Video](#) [News](#) [Maps](#) [more »](#)

digital signature braid group

Search

[Advanced Scholar Search](#)
[Scholar Preferences](#)
[Scholar Help](#)
Scholar All articles - [Recent articles](#) Results **1 - 10** of about **4,020** English pages for **digital signature braid group**. (0.09 seconds)

[New public-key cryptosystem using braid groups- *psu.edu \[PDF\]](#)

KH Ko, SJ Lee, JH Cheon, JW Han, J Kang, C Park - Lecture Notes in Computer Science, 2000 - Springer

 ... Key words: public key cryptosystem, **braid group**, conjugacy problem, key exchange, hard problem, non-commutative **group**, one-way function, public key ...

[Cited by 153](#) - [Related articles](#) - [Web Search](#) - [BL Direct](#) - [All 16 versions](#)

[\[PDF\] *New signature scheme using conjugacy problem](#)

KH Ko, DH Choi, MS Cho, JW Lee - preprint, 2002 - citeseerx.ist.psu.edu

 ... We propose a new **digital signature** scheme based on a non-commutative **group** where the conjugacy ... We implement our **signature** scheme in the **braid** groups and ...

[Cited by 29](#) - [Related articles](#) - [View as HTML](#) - [Web Search](#) - [All 7 versions](#)

[Group Signature Schemes Using Braid Groups- *arxiv.org \[PDF\]](#)

T Thomas, AK Lal - Arxiv preprint cs.CR/0602063, 2006 - arxiv.org

 ... Key Words: **braid group**, **braid** cryptography, **digital signature**, **group signature**

2000 MSC: Primary: 94A60; Secondary: 20F36 1 Introduction ...

[Cited by 6](#) - [Related articles](#) - [View as HTML](#) - [Web Search](#) - [All 3 versions](#)

[New digital signature scheme in Gaussian monoid](#)

E Sakalauskas - Informatica, 2004 - IOS Press

 ... New **Digital Signature** Scheme in Gaussian Monoid ... It is a pure **signature** scheme based on **group** theory mechanism ... p is canonical length and n is **Braid group** index. ...

[Cited by 3](#) - [Related articles](#) - [Web Search](#) - [All 3 versions](#)

[\[PDF\] *A survey of public-key cryptosystems](#)

N Kobitz, AJ Menezes - Siam Review, 2004 - pki.iam.metu.edu.tr

 ... execution of private-key operations such as decryption and **signature** generation. ... longest— and is still the most popular system for electronic commerce—is ...

[Cited by 16](#) - [Related articles](#) - [View as HTML](#) - [Web Search](#) - [BL Direct](#) - [All 16 versions](#)

[\[PDF\] *Post-Quantum Signatures](#)

J Buchmann, C Coronado, M Doring, D Engelbert, C ... - Preprint, 2004 - eprint.iacr.org

 ... So Shor's algorithm breaks all **digital signature** schemes in use ... The **signature** variant of that system is described in ... The n-th **Braid group** B_n is the **group** of ...

[Cited by 4](#) - [Related articles](#) - [View as HTML](#) - [Web Search](#) - [All 12 versions](#)

[One digital signature scheme in semimodule over semiring](#)

E Sakalauskas - Informatica, 2005 - IOS Press

 ... One **Digital Signature** Scheme in Semimodule over Semiring ... When G is a **Braid group**, then the left weighted canonical form transformation could be applied (Ko et ...

[Cited by 4](#) - [Related articles](#) - [Web Search](#) - [All 4 versions](#)

[\[PDF\] *Provably-Secure Identification Scheme based on Braid Group](#)

Z Kim, K Kim - Proceedings of the international conference on soft ..., 2004 - caislab.icu.ac.kr

 ... **group** G, MCSP is feasible if and only if MTSP is feasible. Proof. See the proof

 of 'Theorem 1' in [2] ■ 2.3 Ko et al.'s Conjugacy **Signature** A **braid**- ...

[Cited by 5](#) - [Related articles](#) - [View as HTML](#) - [Web Search](#) - [All 2 versions](#)

[New public key cryptosystem using finite non Abelian groups- •iacr.org \(PDF\)](#)

SH Paeng, KC Ha, JH Kim, S Chee, C Park - Lecture notes in computer science, 2001 - Springer

... to make a **signature** scheme with our PKC: In general, it is not easy to find a **signature** scheme using an infinite non abelian **group** such as a **braid group** [11]. ...

[Cited by 31](#) - [Related articles](#) - [Web Search](#) - [BL Direct](#) - [All 5 versions](#)

[Cryptanalysis of a pseudorandom generator based on braid groups- •saitama-u.ac.jp \(PDF\)](#)

R Gennaro, D Micciancio - Lecture notes in computer science, 2002 - Springer

... 8]. 2 Preliminaries The n -**braid group** B_n is an infinite non-commutative **group** defined by the following **group** presentation: $B_n = \langle \sigma_1, \dots, \sigma_{n-1} \mid \sigma_i \sigma_{i+1} \sigma_i = \sigma_{i+1} \sigma_i \sigma_{i+1}, \sigma_i^2 = 1, 1 \leq i \leq n-1 \rangle$...

[Cited by 5](#) - [Related articles](#) - [Web Search](#) - [BL Direct](#) - [All 10 versions](#)

Key authors: [K Ko](#) - [C Park](#) - [S Lee](#) - [J Cheon](#) - [J Han](#)

Google

Result Page: 1 2 3 4 5 6 7 8 9 10 [Next](#)

digital signature braid group

Search

[Google Home](#) - [About Google](#) - [About Google Scholar](#)

©2009 Google